

PROMOTING

**KNOWLEDGE
MANAGEMENT CULTURE**



DATA PROTECTION



Data Protection and Privacy Act and its implications for research data



Management of personal data across online platforms



Institutional compliance and risk mitigation



GILBERT SSETTUUMA
Legal Officer, Personal Data
Protection Office

November 5th, 2025

11:00 am - 12:00 pm



ID: 913 1040 3130

Passcode: KMseries



www.naro.go.ug



info@naro.go.ug



Personal
DATA
Protection
OFFICE

Data Protection and Privacy Training – NARO

Wednesday, 5th November, 2025

Conducted by: GILBERT SSETTUUMA

Presentation Outline

- The Personal Data Protection Office
- History of Privacy
- Unpacking Data Protection and Privacy
- Incident Response & Breach Management
- Building a Privacy-First Culture
- Q&A



About the Office



Uganda's data protection and privacy regulator



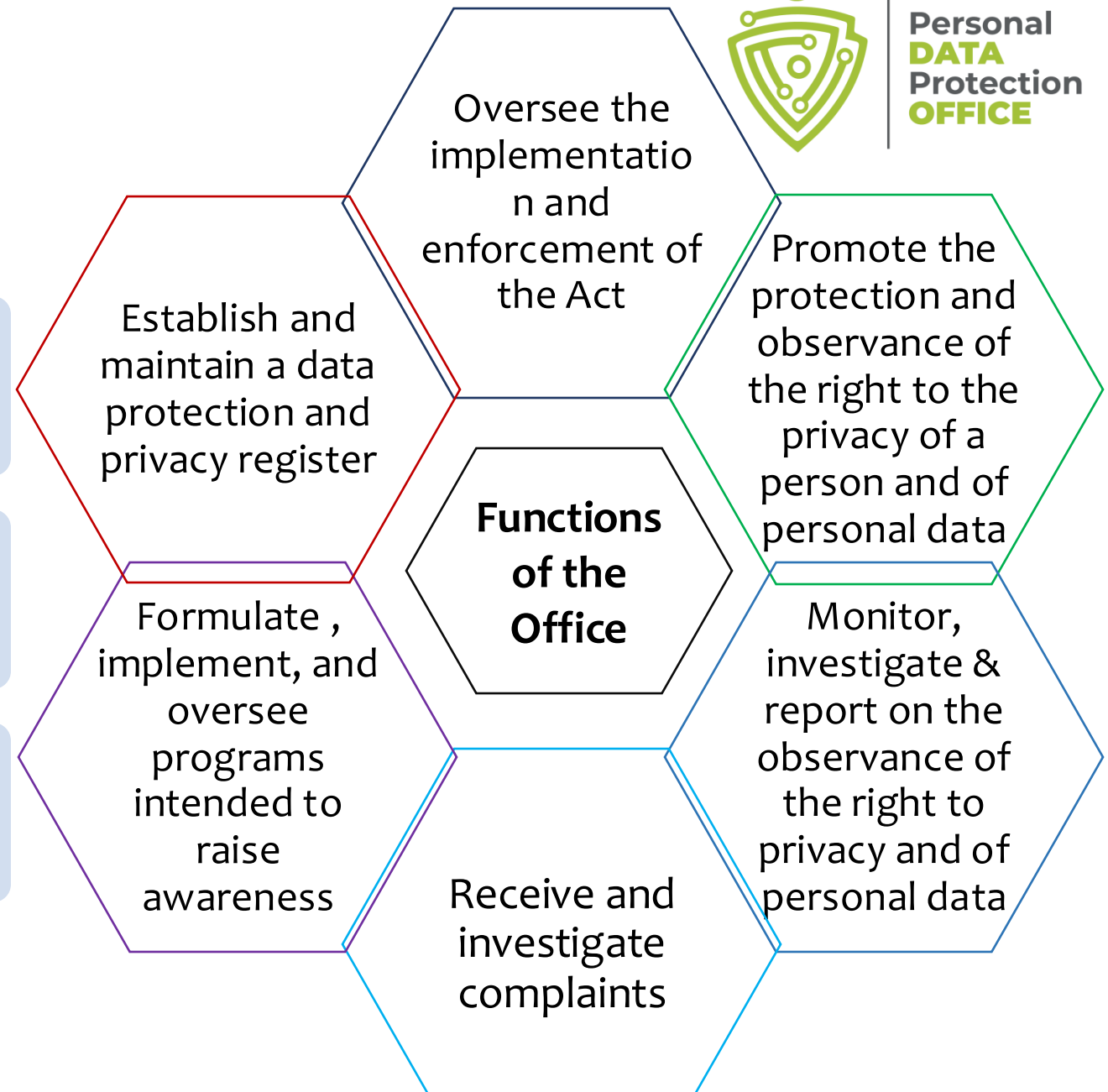
Established in **August 2021** as an independent Office with NITA-U



Mandate: To oversee the implementation of and enforcement of the **Data Protection & Privacy Act, Cap.97**



Personal
DATA
Protection
OFFICE



PDPO Contact Points



@pdpoUganda

- **Location:** Padre Pio House, Plot 32A, Lumumba Avenue
- **Email:** info@pdpo.go.ug
- **Website:** www.pdpo.go.ug
- **Telephone:** 0417-801008/009/011

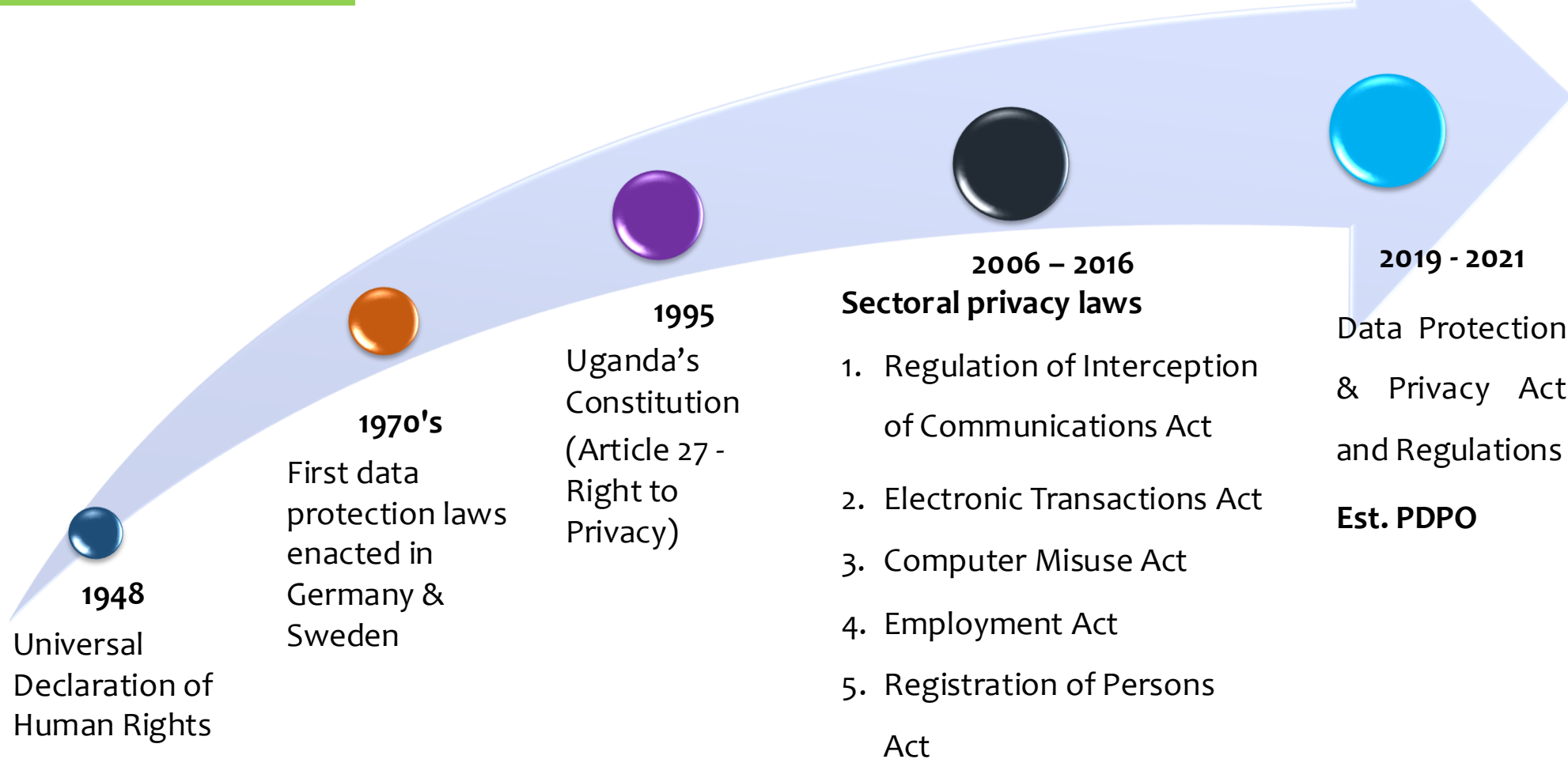
EVOLUTION OF DATA PROTECTION & PRIVACY



Uganda's Data Protection & Privacy Legal Framework



Personal
DATA
Protection
OFFICE





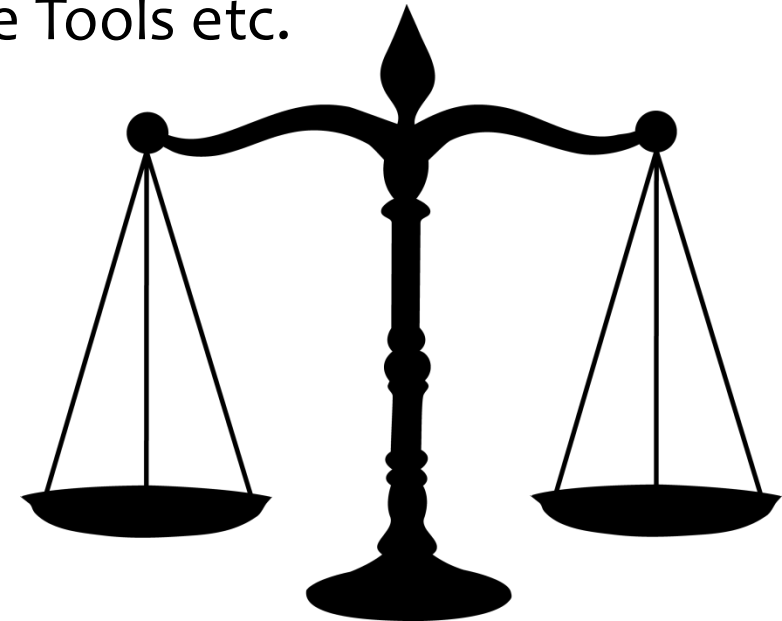
Personal
DATA
Protection
OFFICE

Unpacking Data Protection and Privacy

National Legal Frameworks



- The Constitution 1995 (as amended)
- The Data Protection and Privacy Act, Cap. 97
- The Data Protection and Privacy Regulations, 2021
- PDPO Guidance Notes, Standards, Frameworks, Compliance Tools etc.



Application of the Act



1. Territorial scope

Applies to a person/institution/public body collecting, processing, holding or using personal data within Uganda. It also has an extra-territorial scope that applies to anyone outside Uganda who collects, processes, holds, or uses Ugandan citizens' personal data.

2. Material scope

Applies to personal data processed by automated or non-automated means.



Key Definitions



- **Data Subject:** An individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.
- **Data Controller:** A person who determines the purpose for and the manner in which personal data is processed or is to be processed.
- **Data Processor:** A person other than an employee of the data controller who processes data on behalf of the data controller.
- **Data collector:** An individual, public body or institution that collects personal data.

Key Definitions



- **Data Protection Officer (DPO):** An officer appointed or designated by the data collector, data controller or data processor to be responsible for ensuring compliance with the Act.
- **Consent:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

Personal Data



A company's
Annual Financial
Report



Staff Payroll



Staff Medical
Information



Your name and
date of birth



An anonymous
response to a customer
survey question



CCTV Footage
captured at
NARO offices



“Any Information in any recorded form relating to a living individual from which they can be identified”

Major Categories of Personal Data

General Personal Data

- First/middle name
- Last name
- Address
- Mobile number
- E-Mail address
- Internet Protocol (IP) address
- Date of birth
- Occupation



Sensitive Personal Data

- Race or ethnic origin
- Political, religious or philosophical beliefs
- Trade union membership
- Genetic data or biometric data
- Health information



Personal
DATA
Protection
OFFICE

Obligations of NARO as a Data Controller - 1



- Register with the PDPO
- Establish a Privacy Governance Structure
- Develop Organizational Policies and Procedures on Data Protection & Data Security
- Train Employees on the developed policies and procedures
- Report to PDPO and effectively manage any data breaches
- Submit Annual Compliance Reports to PDPO within 90 days after the end of every financial year
- Take steps to facilitate data subjects to exercise their privacy rights

Obligations of NARO as a Data Controller - 2



- Ensure personal data is collected and processed in accordance with the law.
- Ensure further processing/secondary use of personal data collected is in accordance with the original purpose
- Conduct thorough due diligence before processing personal data out of Uganda – ensure that such jurisdictions have equivalent protection

Principles of Data Protection & Privacy



Personal
DATA
Protection
OFFICE

Internal Accountability Mechanisms



Personal
DATA
Protection
OFFICE



External Stakeholder Accountability



Personal
DATA
Protection
OFFICE

Improved
Compliance



Vendor Management

Due diligence & privacy requirements for third parties



Regular Audits

Independent assessments & compliance monitoring



Customer Communication

Transparent reporting on privacy practices & incidents



Regulatory Engagement

Proactive collaboration with regulatory bodies

Rights of Data Subjects under the Law



**Right to be
Informed**



Right to Access



**Right to
Rectification**



**Right to prevent processing
of personal data for direct
marketing**

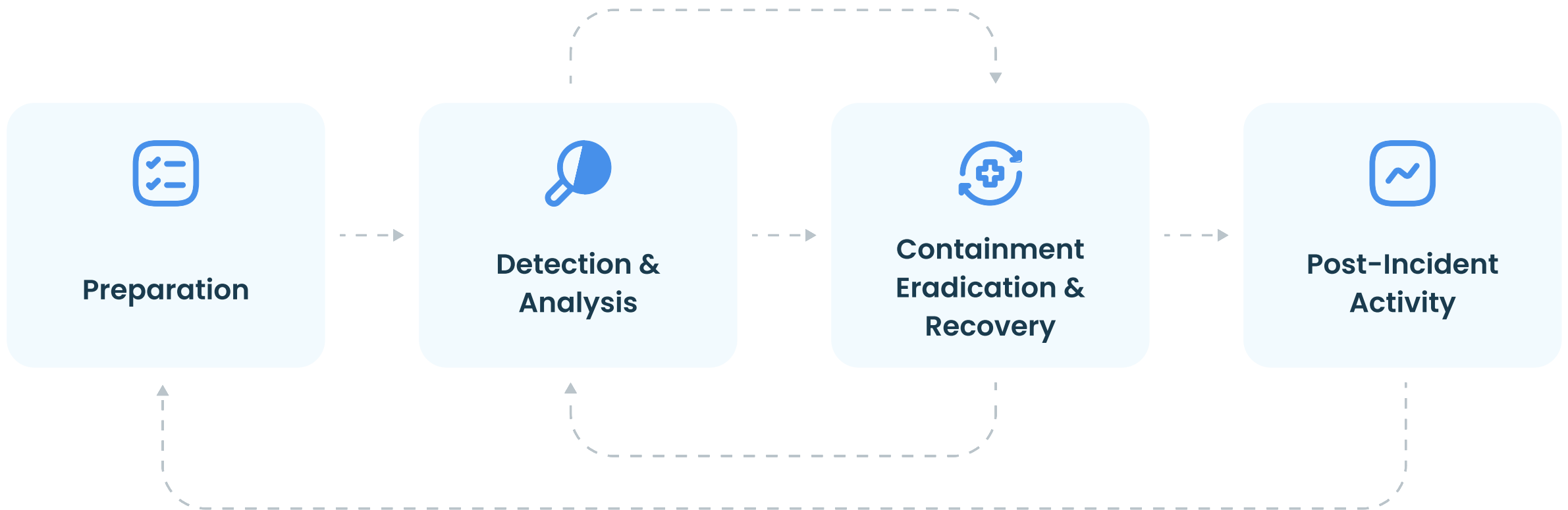


**Right to Erasure
of personal data**

Data Breach Incident Management

- 1. Prepare for a data breach before it happens**
 - Conduct a risk assessment
 - Establish an incident response team
 - Develop a Data Breach Response Plan and sensitize staff on it
 - Train staff on how to recognize a personal breaches
- 2. Detect the data breach**
- 3. Notify PDPO in compliance with the Law**
- 4. Perform urgent incident response actions**
- 5. Gather evidence and analyse the data breach**
- 6. Carry out Containment, Eradication, and Recovery Measures**
- 7. Notify Affected Parties**
- 8. Conduct Post-incident Activities**

Data Breach Incident Management



Team Leader: Responsible for the incident response process and acts as management's primary point of contact (POC).

Lead Investigator: Is the operational head of the incident response operation. This role requires technical expertise and experience with performing incident response activities.



HR/Legal Representation: The incident response team should have HR and Legal representation available to provide guidance and help communicate with stakeholders.

Documentation & Timeline Lead: Ensures that all events and actions are appropriately documented to provide a clear and legally admissible record.

Key Roles on an **Incident Response Team**

When Things Go Wrong



Personal
DATA
Protection
OFFICE



Summary

The Italian data protection authority, Garante, fined Cluster s.r.l. €18,000 for GDPR violations after a complaint about unauthorized disclosure of personal data, including health and criminal data, to third parties and online dissemination. The data was part of educational material for a training event and was inadequately anonymized. Garante found Cluster failed to implement adequate security measures as a data controller, violating GDPR Articles 5(1)(f) and 32(1)(b).

Nation's Largest Rural Lifestyle Retailer to Pay \$1.35M Over CCPA Violations

News: September 30, 2025

SACRAMENTO – The California Privacy Protection Agency (CPPA) Board [has issued a decision](#) requiring Tractor Supply Company, the nation's largest rural lifestyle retailer with more than 2,500 stores in 49 states, to change its business practices and pay a \$1,350,000 fine to resolve claims that the company violated the California Consumer Privacy Act (CCPA). The fine is the largest in the CPPA's history, and the decision is the first to address the importance of CCPA privacy notices and privacy rights of job applicants.

The CPPA opened an investigation into Tractor Supply's privacy practices after receiving a complaint from a consumer in Placerville, California. According to the Board's decision, Tractor Supply violated Californians' privacy rights by:

- Failing to maintain a privacy policy that notified consumers of their rights;
- Failing to notify California job applicants of their privacy rights and how to exercise them;
- Failing to provide consumers with an effective mechanism to opt-out of the selling and sharing of their personal information, including through

New Vision

Probe into data breach at USE complete, says PDPO

The Personal Data Protection Office (PDPO) has concluded its investigation into the data security breach involving the Uganda Securities...

13 Jul 2023



Stabex International Ltd, H.C (Commercial Division) Civil Suit No. 665 of 2021, Court found that Stabex International Ltd had infringed upon its former employee's (Shadia Nalubega) right to privacy when it used her photographs/images for advertising its products on both print and online media without her consent. 16 Jan 2024



Kakuru & Co. Advocates

<https://kakuruadvocates.co.ug> › image-rights-employment ›

Image Rights in Employment - Kakuru & Co. Advocates

Building a Privacy-First Culture (Tips for Staff)

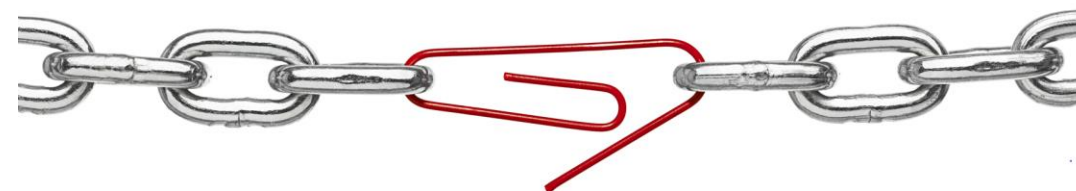


Personal
DATA
Protection
OFFICE

- Acknowledge that you are a target for cyber criminals “The enemy within”
- Practice good password management – **Never share passwords**
- Use free Wi-Fi with caution
- Only browse secure websites (http vs. https)
- Keep your antivirus and malware protection updated
- Beware of phishing scams
- Never leave your device unattended to. Always lock your computer
- Adopt a Clean Desk Policy
- Activate Two Factor or Multi-Authentication (MFA).



Personal
DATA
Protection
OFFICE





Thank You!

